

IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application. An identifier indicating the status of each claim is provided.

Listing of Claims:

1. (Currently Amended) A method of detecting and recovering from violations in a peer-to-peer relay network, comprising:

receiving a first message having first content data at a receiving peer system from a first sending peer system connected to said peer system in a peer-to-peer relay network;

detecting a manipulation of data in said received first message, said manipulation of data changing the outcome of processing by the receiving peer system;

receiving a second message having second content data at the receiving peer system from at least one second sending peer system, wherein the second content data are expected to be substantially the same as the first content data;

wherein detecting the manipulation includes:

comparing by the receiving peer system the received first content ~~and to the received~~ second content data; and

determining that the message from the first sending peer system is different from at least one of the second messages based on the comparison; and

sending a manipulated data alert message to other peer systems connected to said peer system in said peer-to-peer relay network, the manipulated data alert message identifying the first sending peer as responsible for the manipulation of data.

2. – 3. (Canceled)

4. (Currently Amended) A method of detecting and recovering from a cheating violation in a peer-to-peer relay network, comprising:

receiving a message having content data at a receiving peer system from a sending peer system connected to the peer system in a peer-to-peer relay network;

detecting a manipulation of data in the received message, said manipulation of data changing the outcome of processing by the receiving peer system,

wherein detecting said cheating violation includes:

generating predicted data;

comparing by the receiving peer system said message from said sending peer system with said predicted data; and

determining that said message from said sending peer system is different from said predicted data; and

sending a manipulated data alert message to other peer systems connected to said peer system in said peer-to-peer relay network, the manipulated data alert message identifying the sending peer as responsible for the manipulation of data.

5. (Previously Presented) The method of claim 4, further comprising:

sending said predicted data to each other peer system connected to said peer system in said peer-to-peer relay network.

6. (Previously Presented) A method of detecting and recovering from a security violation in a peer-to-peer relay network, comprising:

receiving a message having content data at a receiving peer system from a sending peer system connected to said peer system in a peer-to-peer relay network;

detecting a security violation in said received message, the security violation changing the outcome of processing by the receiving peer system; and

sending a manipulated data alert message to other peer systems connected to said peer system in said peer-to-peer relay network, the manipulated data alert message identifying the sending peer as responsible for the manipulation of data.

7. (Original) The method of claim 6, wherein:

detecting said security violation includes detecting invalid data in said message.

8. (Original) The method of claim 6, wherein:

detecting said security violation includes detecting said message was sent using improper sending procedures.

9. (Original) The method of claim 8, wherein:

said message was sent as part of denial of service attack.

10. (Original) The method of claim 1, further comprising:

ignoring further messages sent by said sending peer system.

11. (Original) The method of claim 1, further comprising:
causing said sending peer system to disconnect from said peer-to-peer relay network.
12. (Previously Presented) The method of claim 1, further comprising:
sending said manipulated data alert message to a server connected to said peer system.
13. (Original) The method of claim 1, further comprising:
the data relayed by peer systems is update data for a network environment.
14. (Original) The method of claim 1, wherein:
the data relayed by peer systems is update data for an online game.
15. (Original) The method of claim 1, wherein:
at least one peer system is a network-enabled game console.
16. (Original) The method of claim 1, wherein:
at least two peer systems are connected through the Internet.
17. (Currently Amended) A receiving peer system in a peer-to-peer relay
network, comprising:
means for receiving a first message having first content data at the receiving peer system
from a first sending peer system connected to said peer system in a peer-to-peer relay network;

means for detecting a manipulation of data in said received first message, said manipulation of data changing the outcome of processing by the receiving peer system;

means for receiving a second message having second content data at the receiving peer system from at least one second sending peer system, wherein the second content data are expected to be substantially the same as the first content data;

wherein detecting said manipulation includes:

comparing by the receiving peer system of the received first content data to the received second content data; and

determining that the first message from the first sending peer system is different from at least one of the second messages based on the comparison; and

sending a manipulated data alert message to other peer systems connected to said peer system in said peer-to-peer relay network, the manipulated data alert message identifying the first sending peer as responsible for the manipulation of data.

18. – 19. (Canceled)

20. (Previously Presented) The peer system of claim 17, further comprising:

means for sending said data manipulation alert message to a server connected to said peer system.

21. (Currently Amended) A computer-readable medium storing a computer-readable program that when executed on a processor ~~cause~~ causes the processor to execute a method in a peer system of a peer-to-peer relay network, the method comprising the steps of:

- receiving a first message having first content data at a receiving peer system from a first sending peer system connected to said peer system in a peer-to-peer relay network
- detecting a manipulation of data in said received first message, said manipulation of data changing the outcome of processing by the receiving peer system;
- receiving a second message having second content data at the receiving peer system from at least one second sending peer system, wherein the second content data are expected to be substantially the same as the first content data;
- wherein detecting the manipulation includes:
 - comparing by the receiving peer system the received first content ~~and to the received~~ second content data; and
 - determining that the message from the first sending peer system is different from at least one of the second messages based on the comparison; and
 - sending a manipulated data alert message to other peer systems connected to said peer system in said peer-to-peer relay network, the manipulated data alert message identifying the first sending peer as responsible for the manipulation of data.

22. - 23 (Canceled)

24. (Previously Presented) The computer-readable medium of claim 21, further comprising sending said data manipulation alert message to a server connected to said peer system.

25. (Canceled)

26. (Previously Presented) A method of detecting and recovering from a violation in a peer-to-peer relay network, comprising:

 sending a first message having first content data from a sending peer system to a receiving peer system;

 detecting a manipulation of data in said sent first message, said manipulation of data changing the outcome of processing by the receiving peer system;

 wherein detecting said manipulation includes:

 relaying back the sent first message to the sending peer by the receiving peer system;

 comparing by the sending peer of the relayed back message to the sent first message to identify a receiving peer responsible for the manipulation of data; and

 sending a manipulated data alert message to other peer systems connected to the peer system in said peer-to-peer relay network, the manipulated data alert message identifying the receiving peer as responsible for the manipulation of data.

27. (Previously Presented) The method of claim 26, further comprising ignoring messages from the sending peer responsible for the manipulation of data.

28. (Previously Presented) The method of claim 26, further comprising forcing the sending peer responsible for the manipulation of data to disconnect from the peer-to-peer relay network.